life.augmented

AN5347

アプリケーション・ノート

# STM32L5 および STM32U5 シリーズの Arm® TrustZone® 機能

## 概要

IoT（モノのインターネット）アプリケーションでは、デバイスはインターネット経由の望ましくない侵入に対して脆弱です。したがって、セキュリティは、デバイスと情報を保護し、信頼できる世界と信頼できない世界を互いに隔離するための重要なトピックです。

STM32L5 および STM32U5 シリーズのデバイス（本書では以降 STM32L5、STM32U5、または STM32L5/U5 と表記します）は、高性能 Arm® Cortex®-M33 32-bit RISC コアをベースにしています。このプロセッサは、Armv8-M アーキテクチャを使用しており、主に、セキュリティが重要な考慮事項となる環境を対象としています。

Armv8-M の Arm® TrustZone® テクノロジーは、ハードウェアをセキュアワールドと非セキュアワールドに分割するように設計されたセキュリティ拡張機能です。Arm® TrustZone® テクノロジーとソフトウェア手法により、STM32L5/U5 マイクロコントローラ（MCU）は、優れた設計の柔軟性を備えたセキュアなアプリケーションを実現します。

本書では、マイクロコントローラのメモリ／リソースをセキュアと非セキュアに分割できる Arm® TrustZone® テクノロジーと STM32L5/U5 デバイスの機能について説明します。

# 1 一般情報

このアプリケーション・ノートは、Arm®Cortex® コアベースのデバイスである STM32L5 および STM32U5 シリーズのマイクロコントローラに適用されます。

注 Arm は、米国内およびその他の地域にある Arm Limited（またはその子会社）の登録商標です。

arm

## 参照文献

[1] リファレンスマニュアル STM32L552xx および STM32L562xx advanced Arm®-based 32-bit MCU（RM0438）

[2] リファレンスマニュアル STM32U575xx および STM32U585xx advanced Arm®-based 32-bit MCU（RM0456）

[3] Armv8-M アーキテクチャ・リファレンスマニュアル（Arm® ウェブサイトから入手可能）

[4] ユーザマニュアル STM32L552ZE マイクロコントローラ搭載評価ボード（UM2597）

[5] ユーザマニュアル STM32U575AII6Q マイクロコントローラ搭載評価ボード（UM2854）

[6] ユーザマニュアル STM32L562QE マイクロコントローラ搭載 Discovery キット（UM2617）

[7] ユーザマニュアル STM32U585AI 搭載 IoT ノード用 Discovery キット（UM2839）

[8] ユーザマニュアル STM32L5 Nucleo-144 ボード（UM2581）

[9] ユーザマニュアル STM32U5 Nucleo-144 ボード（UM2861）

# 2 Arm TrustZone テクノロジー

## 2.1 概要

Armv8-M 用の Arm TrustZone テクノロジーでは、システムを 2 つの領域に分割します。1 つはセキュアワールド、もう 1 つは非セキュアワールドです。

セキュアワールドと非セキュアワールドの分割は、メモリマップに基づいて行われます。

Flash メモリ、SRAM、外部メモリ、ペリフェラル、割込みを含む使用可能なすべてのマイクロコントローラリソースが、セキュアワールドか非セキュアワールドのどちらかに割り当てられます。これらのリソースのセキュリティ属性を計画した後、非セキュアワールドは非セキュアのメモリとリソースにのみアクセスします。一方、セキュアワールドはセキュアと非セキュアリソースを含め、両方のワールドにあるすべてのメモリとリソースにアクセスできます。

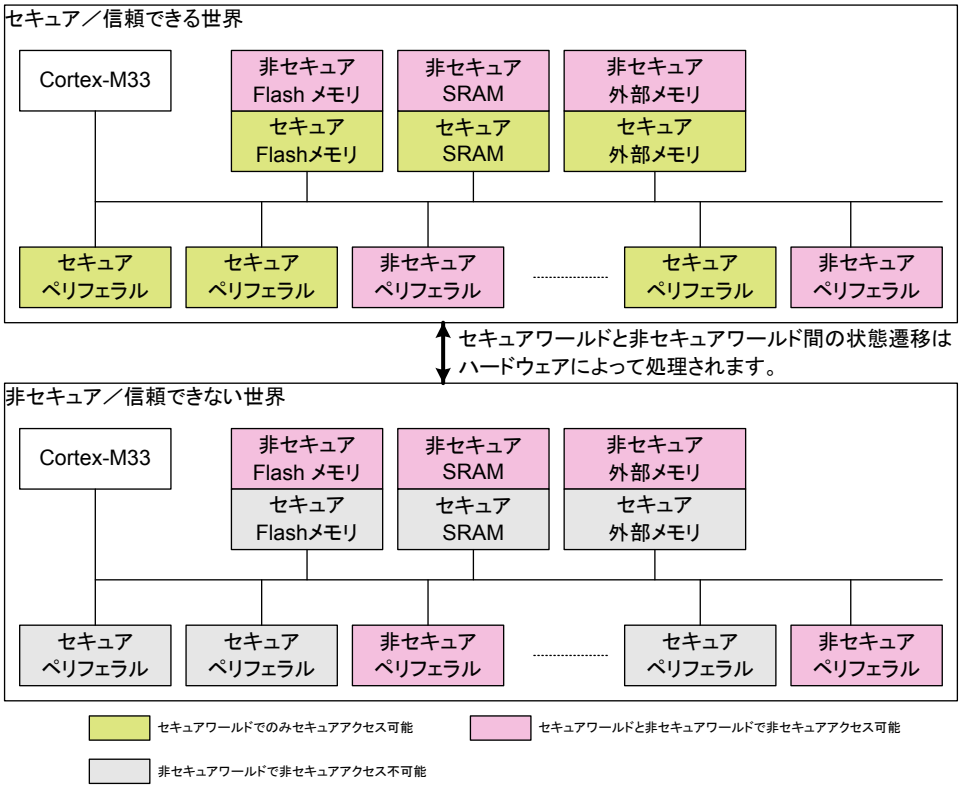
保護が必要な重要データ(暗号キーなど)は、セキュアワールドに置き、そこで安全に処理する必要があります。

コードが実行される場所によって、コードの種類が次のように定義されます。

- コードがセキュアメモリで実行される場合、それをセキュアコードと呼びます。
- コードが非セキュアメモリで実行される場合、それを非セキュアコードと呼びます。

下の図に示すように、セキュアコードと非セキュアコードは同じ STM32L5/U5 デバイス上で動作します。

**図 1. セキュアワールドと非セキュアワールド間のリソース分割**



## 2.2 セキュリティ状態

簡単に言うと、実行されるコードのアドレスによって、CPU のセキュリティ状態、すなわちセキュアか非セキュアかが決まります。

- CPU が非セキュアメモリ内のコードを実行する場合、CPU は非セキュア状態になります。
- CPU がセキュアメモリ内のコードを実行する場合、CPU はセキュア状態になります。

Armv8-M テクノロジーでは、以下のアドレスセキュリティ属性を定義しています。

- セキュア
  セキュアアドレスは、セキュアコードまたはセキュアマスタのみがアクセス可能なメモリとペリフェラルに使用されます。セキュアトランザクションとは、セキュアとして動作しているマスタから発生するトランザクションです。
- 非セキュアから呼出し可能（NSC）
  NSC は、特殊なタイプのセキュア領域です。このタイプのメモリは、Armv8-M プロセッサがそのメモリに対して SG（セキュアゲートウェイ）命令を保持することを許可する唯一のタイプであり、その SG 命令は、ソフトウェアが非セキュア状態からセキュア状態に遷移することを可能にするものです。この SG 命令は、非セキュアアプリケーションが無効なエントリポイントに分岐するのを防ぐために使用できます。
  非セキュアコードがセキュア側の関数を呼び出す場合、
  – API の最初の命令は SG 命令でなければなりません。
  – SG 命令は、NSC 領域内にある必要があります。

  セキュアコードは、非セキュアコードにセキュアなサービスアクセスを提供するために、非セキュアから呼出し可能な関数も提供しています。
- 非セキュア
  非セキュアアドレスは、デバイスで実行されているすべてのソフトウェアからアクセス可能なメモリとペリフェラルに使用されます。非セキュアトランザクションは、非セキュアとして動作しているマスタから、または非セキュアアドレスにアクセスしているセキュアマスタから発生します（データトランザクションのみであり、フェッチ命令ではありません）。非セキュアトランザクションは、非セキュアアドレスへアクセスすることのみ許可されます。非セキュアトランザクションは、セキュアアドレスにはアクセスできません。

# 3 STM32L5 および STM32U5 シリーズでの TrustZone の実装

## 3.1 STM32L5 および STM32U5 TrustZone のアクティブ化

STM32L5/U5 では、TrustZone はデフォルトで無効であり、対応するオプションバイトの TZEN オプションビットをセットすることによって有効になります。

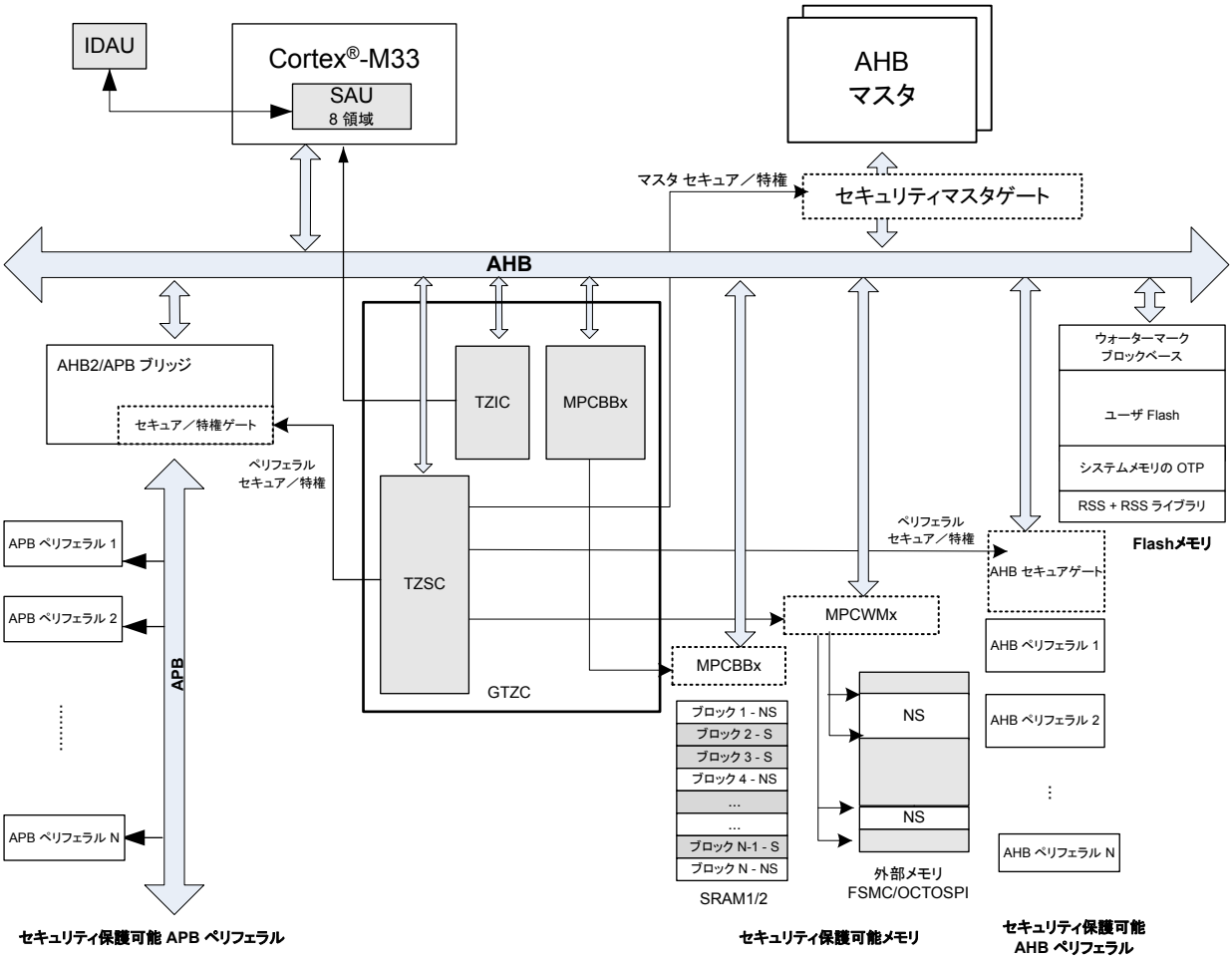
本書で説明されているすべての機能は、TrustZone が有効になっている STM32L5/U5 デバイスに適用されます。

## 3.2 TrustZone ブロック図

STM32L5/U5 では、TrustZone は、SAU（セキュア属性ユニット）、IDAU（実装定義属性ユニット）、Flash メモリ、および GTZC（グローバル TrustZone セキュリティコントローラ）によって実装されます。

次のブロック図に、TrustZone 実装の詳細を示します。

**図 2. STM32L5 および STM32U5 の TrustZone 実装の概要**



## 3.3 セキュア属性ユニット(SAU)と実装定義属性ユニット(IDAU)

CPU から見たメモリアドレスのセキュリティ状態は、内部の SAU(セキュア属性ユニット)と IDAU(実装定義属性ユニット)の組み合わせによって制御されます。

セキュリティ属性の結果は、IDAU と SAU 間のより高いセキュリティ設定です。セキュリティ属性の優先順位は、次のとおりです。

- セキュアには、最も高いセキュア優先順位がありす。
- 非セキュアから呼出し可能は、低いセキュア優先順位です。
- 非セキュアは、セキュア優先順位が最も低くなります。

下の表に、特定のセキュリティ属性(セキュア、非セキュア、または非セキュアから呼出し可能)を特定のアドレスに割り当てる方法を示します。

**表 1. IDAU および SAU を使用したセキュリティ属性の設定**

| IDAU セキュリティ属性 | SAU セキュリティ属性(1) | 最終的なセキュリティ属性 |
|---|---|---|
| 非セキュア | セキュア | セキュア |
| | セキュア - NSC | セキュア - NSC |
| | 非セキュア | 非セキュア |
| セキュアまたは NSC(2) | セキュア | セキュア |
| | 非セキュア | セキュア - NSC |

1. 定義領域は 32 バイト境界に揃えられます。
2. NSC = 非セキュアから呼出し可能

### 3.3.1 STM32L5 および STM32U5 の IDAU とメモリのエイリス化

STM32L5/U5 のメモリ配置では Arm の推奨に従って、重複したメモリマップを実装します。1 つがセキュアビュー用、もう 1 つが非セキュアビュー用です。

つまり、メモリマップの各領域(コード、SRAM、ペリフェラル)は 2 つのサブ領域に分割され、各内部メモリとペリフェラルは、非セキュアビューとセキュアビューとで 2 つの別のアドレス位置でデコードされます。これらの領域のセキュリティ属性を定義するために、IDAU が実装されています。

IDAU のメモリマップのパーティションは設定可能にはなっていません。ハードウェアによって固定されています。下の表に、STM32L5/U5 の IDAU で定義されているメモリマップセキュリティ属性のパーティションを示します。

**表 2. STM32L5 および STM32U5 での IDAU によるメモリマップアドレスのセキュリティ属性**

| 地域 | アドレス範囲 | IDAU によるセキュリティ属性 |
|---|---|---|
| コード - 再配置時の外部メモリ | 0x0000 0000 - 0x07FF FFFF(128 MB) | 非セキュア |
| コード - Flash メモリおよび SRAM | 0x0800 0000 - 0x0BFF FFFF(64 MB) | 非セキュア |
| | 0x0C00 0000 - 0x0FFF FFFF(256 MB) | 非セキュアから呼出し可能 |
| コード - 再配置時の外部メモリ | 0x1000 0000 - 0x1FFF FFFF(256 MB) | 非セキュア |
| SRAM | 0x2000 0000 - 0x2FFF FFFF(256 MB) | 非セキュア |
| | 0x3000 0000 - 0x3FFF FFFF(256 MB) | 非セキュアから呼出し可能 |
| ペリフェラル | 0x4000 0000 - 0x4FFF FFFF(256 MB) | 非セキュア |
| | 0x5000 0000 - 0x5FFF FFFF(256 MB) | 非セキュアから呼出し可能 |
| 外部メモリ(1) | 0x6000 0000 - 0xDFFF FFFF(2 GB) | 非セキュア |

1. 外部メモリ領域にはエイリアスは設定しません。

### 3.3.2 STM32L5 および STM32U5 の SAU

STM32L5/U5 には 8 つの SAU 領域があります。ユーザは、下の表に示すように、必要なセキュリティ設定パーティションを SAU によって変更します。TrustZone が有効な場合、SAU は、デフォルトですべてのアドレスをセキュアとして設定し、すべてのメモリ領域がセキュアと見なされます。

**表 3. STM32L5 および STM32U5 での SAU によるメモリマップアドレスのセキュリティ属性**

| 地域 | アドレス範囲 | IDAU によるセキュリティ属性 | SAU によるセキュリティ属性 | 最終的なセキュリティ属性 |
|---|---|---|---|---|
| コード - 再配置時の外部メモリ | 0x0000 0000 - 0x07FF FFFF | 非セキュア | セキュア<br>非セキュアまたは<br>非セキュアから呼出し可能 | セキュア<br>非セキュアまたは<br>非セキュアから呼出し可能 |
| コード - Flash メモリおよび SRAM | 0x0800 0000 - 0x0BFF FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x0C00 0000 - 0x0FFF FFFF | 非セキュアから呼出し可能 | セキュアまたは<br>非セキュアから呼出し可能 | セキュアまたは<br>非セキュアから呼出し可能 |
| コード - 再配置時の外部メモリ | 0x1000 0000 - 0x1FFF FFFF | 非セキュア | 非セキュア | 非セキュア |
| SRAM | 0x2000 0000 - 0x2FFF FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x3000 0000 - 0x3FFF FFFF | 非セキュアから呼出し可能 | セキュアまたは<br>非セキュアから呼出し可能 | セキュアまたは<br>非セキュアから呼出し可能 |
| ペリフェラル | 0x4000 0000 - 0x4FFF FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x5000 0000 - 0x5FFF FFFF | 非セキュアから呼出し可能 | セキュアまたは<br>非セキュアから呼出し可能 | セキュアまたは<br>非セキュアから呼出し可能 |
| 外部メモリ | 0x6000 0000 - 0xDFFF FFFF | 非セキュア | セキュア<br>非セキュアまたは<br>非セキュアから呼出し可能 | セキュア<br>非セキュアまたは<br>非セキュアから呼出し可能 |

**例**

ペリフェラルは、2 つのアドレス範囲でデコードされます。非セキュアビューでは 0x4000 00000、セキュアビューでは 0x5000 0000 です。

SAU と IDAU のプログラミングに従って、セキュアコードはセキュアトランザクションを生成することで、セキュアビュー内のペリフェラルにアクセスし、非セキュアコードは非セキュアビュー内の別のアドレスにある同じペリフェラルにアクセスします。アクセスは、GTZC/TZSC によってペリフェラルセキュリティ属性がどのように定義されているかに応じて、許可または拒否されます。詳細については、セクション 4 およびセクション 5 を参照してください。

#### STM32CubeL5 および STM32CubeU5 での SAU の設定

SAU 領域の定義は、次の CMSIS ファイルで行います。

- STM32U5：デバイス `partition_stm32U575xx.h` および `partition_stm32U585xx.h`
- STM32L5：デバイス `partition_stm32l552xx.h` および `partition_stm32l562xx.h`

セキュアプロジェクトによって、SAU が有効にされ、SAU 領域が定義されます。STM32CubeL5 および STM32CubeU5 では、下の表に記載されているデフォルトの SAU 領域が定義されます（リンカのメモリレイアウトファイルのテンプレートに関連）。

**表 4. STM32CubeL5 および STM32CubeU5 のデフォルトの SAU 領域**

| SAU 領域 | STM32L5 アドレス | STM32U5 アドレス | STM32Cube SAU |
|---|---|---|---|
| SAU 領域 0 | 0x0C03 E000 - 0x0C03 FFFF | 0x0C0F E000 - 0x0C0F FFFF | セキュア、非セキュアから呼出し可能 |
| SAU 領域 1 | 0x0804 0000 - 0x0807 FFFF（256 KB Flash バンク 2） | 0x0810 0000 - 0x081F FFFF（1 MB Flash バンク 2） | 非セキュア |
| SAU 領域 2 | 0x2001 8000-0x2003 FFFF（SRAM、SRAM1 の後半 160 KB + SRAM2） | 0x2004 0000 - 0x200B FFFF（SRAM3） | |
| SAU 領域 3 | 0x4000 0000 - 0x4FFF FFFF（ペリフェラルにマップされたメモリ） | | |
| SAU 領域 4 | 0x6000 0000 - 0x9FFF FFFF（外部メモリ） | | |
| SAU 領域 5 | 0x0BF9 0000 - 0x0BFA 8FFF（システムメモリ） | | |
| SAU 領域 6 | 未使用 | | |
| SAU 領域 7 | | | |

SAU 領域によってカバーされない 0x0000 0000-0xDFFF FFFF にあるすべてのメモリ空間は、セキュアとして固定されています。

IDAU によって提供されるセキュリティ属性と、SAU によって提供されるセキュリティ属性を組み合わせた結果を下の表に示します。

**表 5. STM32CubeL5 のメモリのセキュリティパーティション分割**

| 地域 | アドレス範囲 | IDAU によるセキュリティ属性 | SAU によるセキュリティ属性 | 最終的なセキュリティ属性 |
|---|---|---|---|---|
| Flash メモリ | 0x0804 0000 - 0x0807 FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x0C00 0000 - 0x0C03 DFFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| | 0x0C03 E000 - 0x0C03 FFFF | 非セキュアから呼出し可能 | 非セキュアから呼出し可能 | 非セキュアから呼出し可能 |
| SRAM1 | 0x3000 0000 - 0x3001 7FFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| | 0x2001 8000 - 0x2002 FFFF | 非セキュア | 非セキュア | 非セキュア |
| SRAM2 | 0x2003 0000 - 0x2003 FFFF | 非セキュア | 非セキュア | 非セキュア |
| ペリフェラル | 0x4000 0000 - 0x4FFF FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x5000 0000 - 0x5FFF FFFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| 外部メモリ | 0x6000 0000 - 0x9FFF FFFF | 非セキュア | 非セキュア | 非セキュア |

表 6. STM32CubeU5 のメモリのセキュリティパーティション分割

| 地域 | アドレス範囲 | IDAU によるセキュリティ属性 | SAU によるセキュリティ属性 | 最終的なセキュリティ属性 |
|---|---|---|---|---|
| Flash メモリ | 0x0810 0000 - 0x081F FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x0C00 0000 - 0x0C0F DFFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| | 0x0C0F E000 - 0x0C0F FFFF | 非セキュアから呼出し可能 | 非セキュアから呼出し可能 | 非セキュアから呼出し可能 |
| SRAM1 | 0x3000 0000 - 0x3002 7FFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| SRAM2 | 0x3003 0000 - 0x3003 FFFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| SRAM3 | 0x2004 0000 - 0x200B FFFF | 非セキュア | 非セキュア | 非セキュア |
| SRAM4 | 0x2800 0000 - 0x2800 3FFF | 非セキュア | 非セキュア | 非セキュア |
| ペリフェラル | 0x4000 0000 - 0x4FFF FFFF | 非セキュア | 非セキュア | 非セキュア |
| | 0x5000 0000 - 0x5FFF FFFF | 非セキュアから呼出し可能 | セキュア | セキュア |
| 外部メモリ | 0x6000 0000 - 0x9FFF FFFF | 非セキュア | 非セキュア | 非セキュア |

これはもちろん一例です。ユーザは、セキュアおよび非セキュアリソースに関するアプリケーション要件に基づいて、メモリ分割を調整する必要があります。

# 4 STM32L5 および STM32U5 シリーズのセキュリティ設定

SAU/IDAU 設定は、1 つのマスタ（CPU）にのみ適用されます。他のマスタ（DMA など）はこれらのポリシーを認識しません。このため、ペリフェラル側にローカルセキュアゲートが必要です。

STM32L5/U5 デバイスには、Cortex-M33 TrustZone 機能に加え、SAU/IDAU に重ねて 2 番目のレベルのセキュリティを提供することによって、セキュアワールドと非セキュアワールド間のより柔軟性の高い分割を強化・可能にする補足的なセキュリティ機能が搭載されています。

## 4.1 Flash メモリのセキュリティ設定

Flash メモリ領域は、IDAU/SAU によって非セキュアとなっている場合でも、不揮発性 Flash セキュアウォーターマークと揮発性ブロックベースの Flash インタフェースレジスタにより、セキュアとして設定できます。

SAU と IDAU は、CPU によって発行されたトランザクションを許可し、相互接続への CPU アクセスにセキュアまたは非セキュアのタグを付けます。Flash メモリのセキュアウォーターマークとブロックベースのレジスタは、CPU/Cortex-M33 および以下のようなその他のマスタからのトランザクションを許可します。

- STM32L5 のマスタ：DMA1、DMA2、および SDMMC
- STM32U5 のマスタ：GPDMA1（2 つのマスタポートを備えた汎用 DMA）、DMA2D、SDMMC1、および SDMMC2

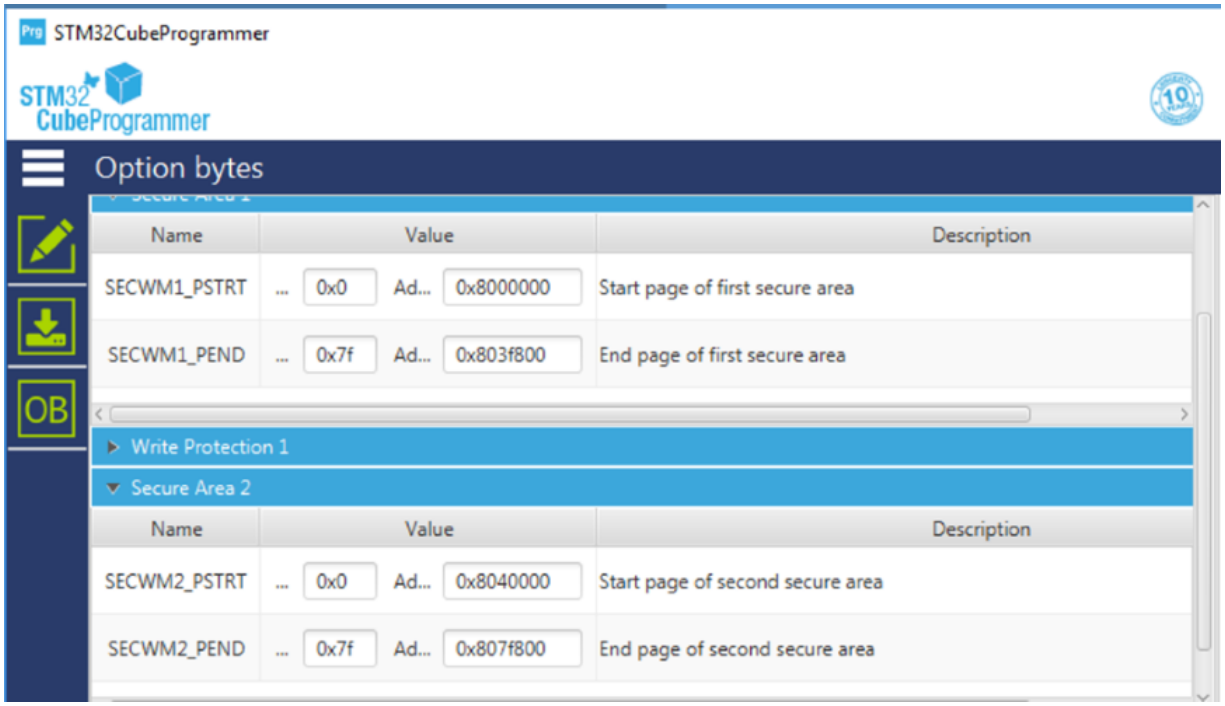
図 2 に示したように、Cortex-M33 によって発行された、Flash メモリをターゲットとした各トランザクションは、最初に IDAU/SAU によってチェックされ、次に Flash セキュアウォーターマークまたはブロックベースレジスタによってチェックされます。詳細については、図 5 を参照してください。

### 4.1.1 Flash メモリのセキュアウォーターマーク

オプションバイト SECWMx_PSTRT および SECWMx_PEND（x = 1、2）で、最大 2 つの異なる不揮発性セキュア領域を定義すると、その領域はセキュアアクセスによってのみ読出しまたは書込みが行われます。

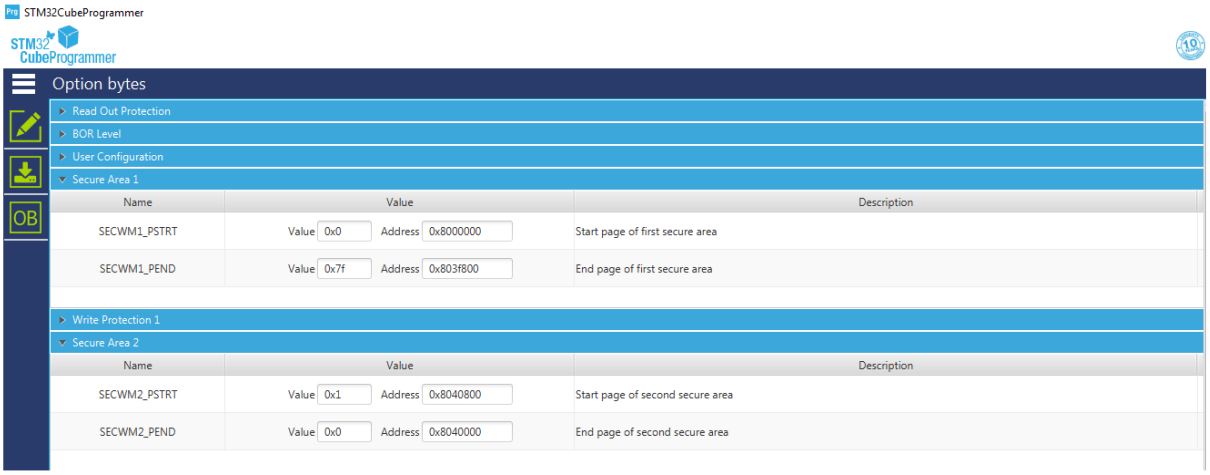
下の図に、TZEN をセットした後のデフォルト値を示します（Flash メモリ全体がセキュア）。

**図 3. TZEN セット後のオプションバイトによるデフォルトの Flash メモリの状態**



STM32CubeL5 および STM32CubeU5 の TrustZone の例では、バンク 1 がセキュアであり、バンク 2 が非セキュアであると想定しています。

**図 4. STM32Cube によってオプションバイトを介して定義されたデフォルトの Flash バンクのセキュリティ状態**




### 4.1.2 Flash メモリブロックベース機能

IDAU/SAU および Flash セキュアウォーターマークオプションバイトによって、Flash メモリ全体が非セキュアになっている場合でも、Flash メモリブロックベース機能を使用して一時的なセキュア領域を設定することができます。

Flash インタフェースブロックベースの設定レジスタを使用して、任意のページをセキュアまたは非セキュアモードにプログラムできます。

ブロックベースレジスタでは、ページが Flash セキュアウォーターマークオプションバイトによって非セキュアに設定されている場合に、そのページをセキュアとして設定することのみできます。反対は不可能です。ページが Flash セキュアウォーターマークオプションバイトによってセキュアとして設定されている場合に、ブロックベースレジスタを使用してそのページを非セキュアとして設定することはできません。

## 4.2 グローバル TrustZone コントローラ（GTZC）

GTZC は、以下のようなサブブロックを備えています。

- TZSC（TrustZone セキュリティコントローラ）では、以下のセキュリティ属性を設定できます。
  - ペリフェラル（下の注を参照）のセキュアまたは非セキュア
  - 外部メモリ：ウォーターマークメモリ保護コントローラ経由（MPCWMx、x = 1、2、3）
- MPCBBx（ブロックベースメモリ保護コントローラ）では、SRAM ブロックのセキュリティ属性を次のように設定できます。
  - STM32L5：SRAM1 および SRAM2 は、MPCBB を使用して、ブロックベースでセキュアまたは非セキュアとしてプログラムできます。ブロックベースのセキュア SRAM の最小単位は、256 バイトのページ単位です。
  - STM32U5：SRAM1、SRAM2、SRAM3、SRAM4 は、MPCBBx を使用して、ブロックごとにセキュアまたは非セキュアとしてプログラムできます。ブロックベースのセキュア SRAM の最小単位は、512 バイトのページ単位です。
- TZIC（TrustZone 不正アクセスコントローラ）は、システム内のすべての不正アクセスイベントを収集し、NVIC に対してセキュア割込み（GTZC_IRQn）を生成します。

注 TrustZone セキュリティが有効な場合、ペリフェラルはセキュリティ保護可能または TrustZone 対応のどちらかになります。

- セキュリティ保護可能：セキュリティ属性は GTZC/TZSC コントローラによって設定されます。
- TrustZone 対応：セキュリティ属性は、一部のペリフェラルセキュアレジスタを使用して設定します。たとえば、GPIO は GPIOx_SECCFGR セキュアレジスタで設定されたセキュリティ属性を持つ TrustZone 対応となります。

セキュリティ保護可能なペリフェラルおよび TrustZone 対応ペリフェラルのリストについては、文書 [1] または [2] の「TrustZone ペリフェラルの分類」セクションを参照してください。

# 5 システム全体のセキュリティアクセスルール

## 5.1 デフォルトのセキュリティ状態

TrustZone セキュリティが Flash_OPTR の TZEN オプションビットで有効化された場合、各システムのデフォルトのセキュリティ状態は以下のとおりです。

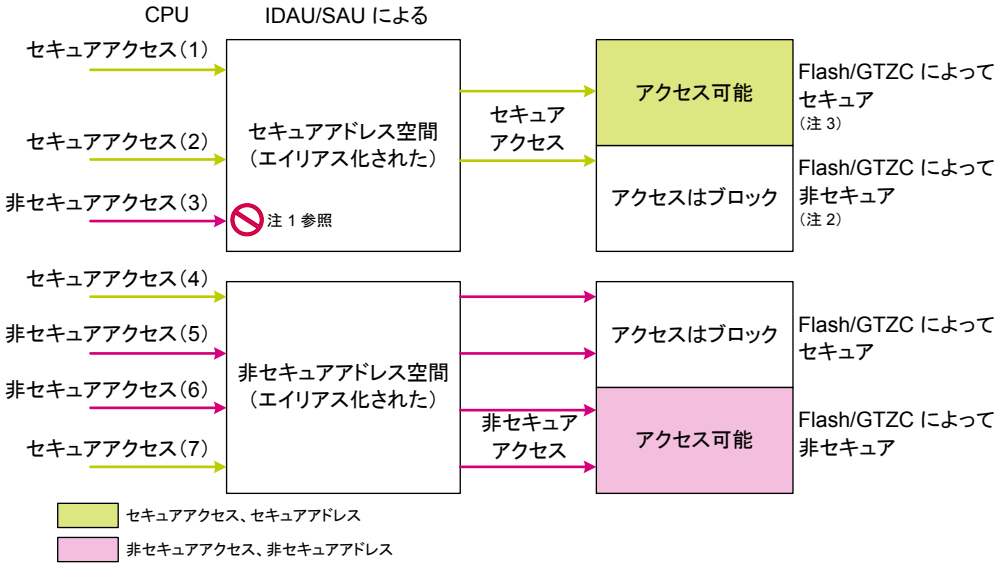
- Cortex-M33 CPU は、リセット後はセキュアな状態です。ブートアドレスは、セキュアメモリ領域を指す必要があります。
- すべての割込みはセキュア割込みコントローラに割り当てられます。
- セキュアコードによって SAU が有効化されて非セキュアリソースの領域が定義されるまで、すべてのメモリマップは IDAU/SAU によって完全にセキュアになっています。
- Flash メモリ全体はセキュアです。セキュリティ領域はウォーターマークユーザオプションバイトによって定義されますが、出荷時の値は次のとおりです。
  - SECWMx_PSTRT = 0x00
  - SECWMx_PEND (x = 1,2) = 0x7F
- すべての SRAM はセキュアです。
- 外部メモリ：FSMC および OCTOSPIx バンクはセキュアです。
- STM32U5 の場合、バックアップ SRAM はセキュアです。
- すべてのペリフェラル（GPIO を除く）は非セキュアです。
- すべての GPIO はセキュアです。
- すべての DMA チャネルは非セキュアです。
- バックアップレジスタは非セキュアです。

## 5.2 メモリとペリフェラルのセキュリティアクセスルール

CPU によって発行されたトランザクションは、最初に SAU でフィルタリングされ、次に、対象のペリフェラル（Flash メモリ、SRAM、外部メモリ、または任意のセキュアペリフェラル）の近くに実装されたセキュアゲートによってフィルタリングされます。

トランザクションのセキュリティ属性に従ったトランザクションのフィルタリングを次の図に示します。

**図 5. メモリおよびペリフェラルのデータアクセスルールの概要**




注：1. アクセスが SAU/IDAU によってブロックされると、セキュアフォールトが発生します。
2. ペリフェラルの非セキュアレジスタには、セキュアトランザクションでもアクセスできます。
これは、メモリアクセスルールとは異なります。また、GTZC_MPCBBx_CR レジスタの SRWILADIS ビットがセットされていると、非セキュア SRAM ブロックでの、セキュア読出し／書込みアクセスが許可されます。
3. Flash/GTZC によるセキュア／非セキュアとは、Flash セキュアウォーターマークオプションバイト、Flash メモリのブロックベースレジスタ、MPCWMx、MPCBB、および TZSC_SECCFGRx レジスタによるセキュリティ属性を指します。

トランザクションにはそれぞれセキュア属性が付いています。これらの属性に応じて、アクセスが許可されるかどうかはSAU によって、次に Flash メモリまたは GTZC（SRAM、外部メモリ、ペリフェラルの場合）によって行われます。

注 STM32L5 の場合のみ、非セキュア情報ブロックには非セキュアトランザクションからのみアクセスできます。情報ブロックとは、オプションバイト、メモリ保護のユーザ設定、システムメモリ、および OTP（ワンタイムプログラマブル）領域で構成される Flash メモリ領域です。特に、OTP 領域、VREFINT、および温度センサ補正値には、非セキュアトランザクションによってのみアクセスされます。したがって、セキュアアプリケーションは、この領域を非セキュアとして設定しているSAU 領域をプログラムしなければなりません。

アクセスルールを以下に示します。

- SAU/IDAU によってセキュアで、かつ Flash/GTZC によってセキュアであるアドレスへのセキュアアクセス：アクセスは許可されます。図 5 の（1）を参照。
- SAU/IDAU によってセキュアで、Flash/GTZC では非セキュアであるアドレスへのセキュアアクセス：アクセスはブロックされます。図 5 の（2）を参照。
- SAU/IDAU によってセキュアであるアドレスへの非セキュアアクセス：Flash/GTZC によるアドレスのセキュリティ属性にかかわらず、アクセスはブロックされます。Cortex-M33 のセキュアフォールト例外がトリガされます。図 5 の（3）を参照。
- SAU/IDAU によって非セキュアであり、Flash/GTZC ではセキュアであるアドレスへのセキュアアクセス：アクセスはブロックされます。図 5 の（4）を参照。
- SAU/IDAU によって非セキュアであり、Flash/GTZC ではセキュアであるアドレスへの非セキュアアクセス：アクセスはブロックされます。図 5 の（5）を参照。
- SAU/IDAU によって非セキュアであり、かつ Flash/GTZC によって非セキュアであるアドレスへの非セキュアアクセス：アクセスは許可されます。図 5 の（6）を参照。
- SAU/IDAU によって非セキュアであり、かつ Flash/GTZC によって非セキュアであるアドレスへのセキュアアクセス：アクセスは許可されます。図 5 の（7）を参照。

アクセスがブロックされた場合、結果は以下のいずれかになります。

- RAZ/WI（ゼロとして読出し／書込みは無視）
- RAZ/WI および不正アクセスイベント／割込み
- バスエラー

たとえば、Flash メモリのセキュア領域への非セキュアアクセスは RAZ/WI となり、不正アクセスイベントが発生します。STM32L5 では GTZC_TZIC_IER2、STM32U5 では GTZC_TZIC_IER4 の FLASHIE によって不正アクセス割込みが有効にされている場合、不正アクセス割込みが生成されます。

詳細については、文書 [1] または [2] を参照してください。

命令フェッチの場合、SAU からのトランザクション出力（セキュアまたは非セキュア）は、CPU の状態には関係なく、ターゲットアドレスに依存します。

**表 7. 命令フェッチルール**

| CPU の状態 | IDAU/SAU によるターゲットメモリアドレスのセキュリティ属性 | トランザクション |
|---|---|---|
| セキュアまたは非セキュア | 非セキュア | 非セキュア |
| セキュアまたは非セキュア | 非セキュアから呼出し可能 | セキュア |
| セキュアまたは非セキュア | セキュア | セキュア |

# 6 ブートおよびルートセキュアサービス（RSS）

RSS は、セキュア Flash メモリ領域の一部であるセキュア情報ブロックに埋め込まれており、ST の生産時にプログラムされます。詳細については、文書 [1] または [2] を参照してください。

RSS では、たとえば RSS 拡張ファームウェア（RSSe SFI）によって、セキュアなファームウェアインストール（SFI）ができます。この機能により、お客様は、信頼できないサードパーティに生産を委託する場合に、STM32 デバイスにプロビジョニングされるファームウェアの機密を保護できます。詳細については、アプリケーション・ノート セキュアファームウェアインストール（SFI）の概要（AN4992）を参照してください。

ブートメモリアドレスは、SECBOOTADD0[24:0] オプションバイトでプログラムします。ただし、許容されるアドレス空間は、Flash メモリの読出し保護（RDP）レベルに依存します。RDP レベルが 0.5 以上で、プログラムされたブートメモリアドレスが許容されるメモリマップ領域外にある場合、デフォルトのブートフェッチアドレスはセキュアなシステム Flash メモリに強制されます。

**表 8. RDP 保護レベルに対するブート領域**

| RDP レベル | ブートアドレス |
|---|---|
| 0 | 任意のブートアドレス |
| 0.5 | RSS またはセキュア Flash メモリのみ |
| 1 | |
| 2 | |

TZEN オプションビットをセットすることによって TrustZone が 有効化されている場合、ブート領域はセキュア領域になければなりません。SECBOOTADD0[24:0] オプションバイトは、セキュアブートメモリアドレスを選択するために使用します。セキュリティを強化して信頼の起点（RoT）を確立するには、他のブートオプションに関係なく、固有のブートエントリオプションを選択する必要があります。このためには、FLASH_SECBOOTADD0R レジスタの BOOT_LOCK オプションビットをセットします。このビットは、セキュアアクセスによってのみセットする必要があります。

注意 STM32L5 の場合、BOOT_LOCK オプションビットは、一度セットするとクリアできません。固有のブートエントリアドレスは、SECBOOTADD0[24:0] オプションバイトでプログラムされたアドレスです。STM32U5 の場合、BOOT_LOCK は RDP レベル 0 でクリアできます。

# 7 TrustZone が有効な場合の読出し保護(RDP)

TrustZone が有効な場合(TZEN = 1)、保護なし(レベル 0)からデバッグ不可の最大保護(レベル 2)までの 4 つの RDP レベルを下の表に示します。

**表 9. RDP 保護レベル(TrustZone が有効な場合)**

| RDP バイト値 | RDP レベル |
|---|---|
| 0xAA | 0 |
| 0x55 | 0.5 |
| 0x55、0xAA、0xCC 以外のすべての値 | 1 |
| 0xCC | 2 |

## 7.1 RDP レベル 1

RDP レベル 1 では、Flash メインメモリ、バックアップレジスタ、バックアップ RAM(STM32U5 のみ)、OTFDEC 領域(使用できる場合)、ICACHE、DCACHE、および SRAM にアクセスできません。CPU がセキュア状態にあるときにデバッグアクセスが行われると、侵入が検出されます。

CPU が非セキュア状態の場合、JTAG/SWD を介したターゲットへの接続および RDP 解除が可能です。CPU の停止以外のデバッグアクセスは、侵入と見なされます。

RDP 解除は、以下のいずれかの方法で行う必要があります。

- ブートローダ経由:ブートは RSS から行う必要があります。
  注:RSS からのブートでは、JTAG/SWD からの解除も可能です。
- JTAG/SWD を介して、ユーザ Flash メモリからのブート:CPU は、ターゲットに接続できるように非セキュア状態である必要があります。
  RDP レベル 1 をプログラミングする前に、ユーザは、セキュアアプリケーションが非セキュアアプリケーションを呼び出すこと(ターゲットへの接続の可能性)、および RDP レベル 1 からの解除が可能であることを確認する必要があります。

注意 非セキュアコードがない場合、CPU は常にセキュア状態に保持され、ユーザ Flash メモリからのブートで、JTAG/SWD を介して RDP を解除することはできません。この場合、解除を行う唯一の方法は、RSS からのブートを使用して JTAG/SWD/ブートローダを使用することです。詳細については、文書 [1] または [2] の「ブート設定」セクションを参照してください。STM32U5 では、RDP レベル 1 の解除は、より低い RDP レベルでプロビジョニングされた OEM1 および OEM2 キーによって保護できます(詳細については、文書 [2] を参照)。

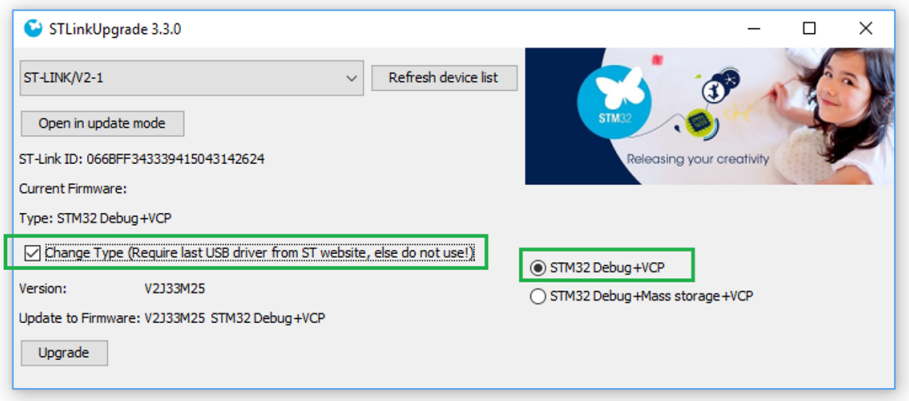
STM32L5/U5 の ST ボード(Nucleo、Evaluation、および Discovery キット)には、同時に電源としてもデバッグにも使用できる ST-LINK が統合されています。ST-LINK 起動(SWD 接続)時にターゲット識別が必要な ST-LINK のマスストレージインタフェースのために、ST-LINK USB ケーブルが接続されるたびにデバッグ侵入が検出されます。侵入が発生した場合、ユーザアプリケーションが実行されることはなく、CPU は常に LOCKUP 状態に保持され、コードを実行することもできません。よって、ターゲットに接続できません。

ユーザアプリケーションの実行を維持し、JTAG/SWD を介してターゲットに接続するには、以下の解決策を使う必要があります。

- ST-LINK はデバッグにのみ使用します。つまり、別の電源ソースを使用する必要があります。ST-LINK USB ケーブルがすでに接続された状態で、ユーザアプリケーションを実行するには、電源をオフ/オンする必要があります。
- 図 6 に示すように、STLinkUpgrade アプリケーションからファームウェアタイプを変更することによって、ST-LINK のマスストレージインタフェースを無効にします。

注 マスストレージを無効にする機能は、ST-Link/V2 にのみ実装されています。

図 6. ST-LINK のマスストレージインタフェースの無効化




## 7.2 RDP レベル 0.5

RDP レベル 0.5 では、セキュア Flash メモリ、セキュアバックアップレジスタ、バックアップ RAM（STM32U5 のみ）、OTFDEC 領域（使用できる場合）、ICACHE、DCACHE、および SRAM 領域にアクセスできません。非セキュア Flash メモリ、非セキュアバックアップレジスタ、および非セキュア SRAM 領域はアクセス可能なままです。

CPU がセキュア状態の場合、JTAG/SWD を介してターゲットに接続することはできません。

CPU が非セキュア状態の場合、JTAG/SWD を介したターゲットへの接続および RDP 解除が可能です。

注 STM32U5 では、RDP レベル 0.5 で、RDP レベル 0 をリクエストできません。RDP をレベル 1 に上げた後に、レベル 0 へ RDP 解除する必要があります。

RDP 解除は、次のいずれかの方法で実行します。

- ブートローダ経由：ブートは RSS から行う必要があります。
  注：RSS からのブートでは、JTAG/SWD からの解除も可能です。
- JTAG/SWD を介して、ユーザ Flash メモリからのブート：RDP レベル 0.5 ではセキュアデバッグは禁止されているため、ターゲットに接続できるようにするには、CPU が非セキュア状態である必要があります。CPU が非セキュア状態のときのみターゲットに接続できるようになります。
  RDP レベル 0.5 をプログラミングする前に、ユーザは、セキュアアプリケーションが非セキュアアプリケーションを呼び出すこと（ターゲットへの接続の可能性）、および RDP レベル 0.5 からの解除が可能であることを常に確認する必要があります。

注意 非セキュアコードがない場合、CPU は常にセキュア状態に保持され、ユーザ Flash メモリからのブートで、JTAG/SWD を介して RDP を解除することはできません。この場合、解除を行う唯一の方法は、RSS からのブートを使用して JTAG/SWD/ブートローダを使用することです。詳細については、文書 [1] または [2] の「ブート設定」セクションを参照してください。

さまざまな読出し保護レベルと、TZEN = 1 の場合のアクセスステータスと保護レベルおよび実行モードの詳細については、文書 [1] または [2] を参照してください。

注 RDP レベル 1 および 0.5 では、STM32CubeProgrammer を使用する場合、ターゲットへの接続は「ホットプラグ」モードで実行する必要があります。ターゲットへの接続中にユーザアプリケーションの実行を維持するためと、CPU がリセット状態の時に（CPU セキュアを意味します）接続されることを避けるためです。

注意 以下の条件が満たされる場合、RDP 解除を行うことはできません。

- BOOT_LOCK オプションビットがセットされている。
- SECBOOTADD0[24:0] はセキュアユーザ Flash メモリ内のアドレスである。
- 非セキュアコードがない。CPU は常にセキュア状態にあり、RDP レベル 0.5 で非セキュア Flash メモリをプログラムすることができない。

## 7.3 RDP レベル 2

RDP レベル 2 がセットされた場合、保護レベル 1 が保証されます。SRAM からのブート（ブート RAM モード）およびシステムメモリからのブート（ブートローダモード）は使用できません。メイン Flash メモリまたは RSS からのブートのみが可能です。

メイン Flash メモリまたは RSS からブートする場合は、メイン Flash メモリ上でのすべての操作が許可されます。ユーザコードからの Flash メモリおよび SRAM に対する読出し、消去、プログラムアクセスが許可されます。

STM32U5 の場合のみ、OEM2 キーがプロビジョニングされていない場合、以下の機能が適用されます。

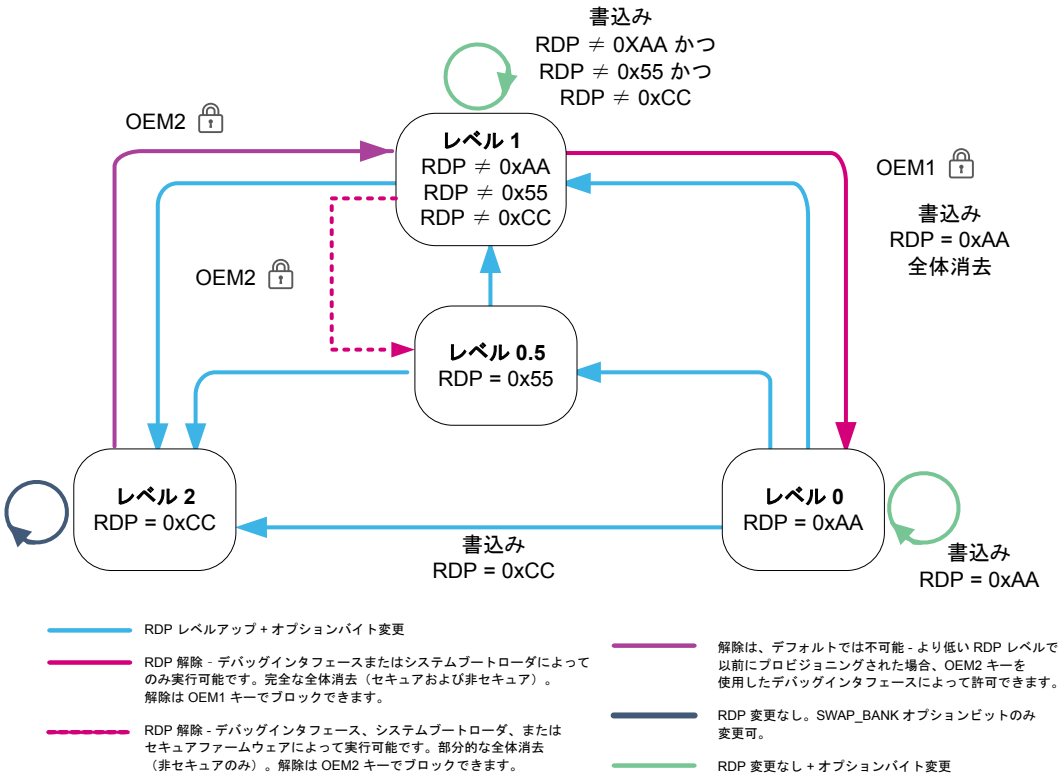
- SWAP_BANK ビットを除くすべてのオプションバイトはプログラムも消去もできません。
- RDP レベル 2 は削除できません（不可逆操作です）。
- すべてのデバッグ機能が無効になります。リセット後も、デバッグは無効になります。
- JTAG と SWD は完全に無効化されます。リセットモードで JTAG/SWD を使用して解除することは可能です。

注 STM32U5 では、より低い RDP 保護下で OEM2 キーが提供されている場合、JTAG と SWD はリセット時のみ有効のままとなります。この目的は、DBGMCU_SR、DBGMCU_DBG_AUTH_HOST、および DBGMCU_DBG_AUTH_DEVICE レジスタとインタフェースし、デバイス識別を取得し、RDP 解除をリクエストするためにこの OEM2 キーを提供するためです。

## 7.4 OEM キーを使用した RDP 遷移（STM32U5 のみ）

下の図に、TrustZone が有効（TZEN = 1）の場合の RDP レベルの遷移図を示します。

**図 7. TrustZone が有効な場合の RDP レベル遷移図**



RDP 解除をロックするために、2 つの 64 ビットキー(OEM1KEY および OEM2KEY)を定義できます(TrustZone の有無にかかわらず使用可能)。

- OEM1KEY は次の状態で変更できます。
  - RDP レベル 0 の状態
  - OEM1LOCK ビットがクリアされている場合は、RDP レベル 0.5 または レベル 1 の状態
- OEM2KEY は次の状態で変更できます。
  - RDP レベル 0 またはレベル 0.5 の状態
  - OEM2LOCK ビットがクリアされている場合は、RDP レベル 1 の状態

解除を実行するには、JTAG または SWD によって OEMxKEY[31:0]、次に OEMxKEY[63:32] を DBGMCU_DBG_AUTH_HOST レジスタにシフトします。キーが OEM2KEY と一致した場合、RDP2 の解除がハードウェアによって起動されます。

詳細については、セクション 10 および文書 [2] を参照してください。

# 8 TrustZone が有効な場合にのみ使用可能なセキュリティ機能

以下の機能は、TrustZone が有効な場合のみ使用できます。

- GTZC セキュアウォーターマーク保護
- HDP（非表示保護）オプションバイト
- Flash メモリのブロックベースセキュア保護
- RDP レベル 0.5
- RSS および SFI
- BOOT_LOCK
- セキュア割込み
- GTZC セキュア保護

# 9 TrustZone の無効化

セクション 2.1 で説明したように、TrustZone は、すべての STM32L5/U5 デバイスで、デフォルトで無効になっています。TrustZone は、TZEN オプションビットをセットすることによって有効化されます。

TrustZone の無効化は、RDP 解除と並行に実行する必要があります（セクション 7.2 参照）。ここでは、システムがすでに RDP レベル 1 または RDP レベル 0.5 であるものとします（レベル 0.5 からの解除は STM32L5 にのみ適用されます）。考慮すべき関連推奨事項については セクション 7.1 および セクション 7.2 を参照してください。

TrustZone を無効化すると、セクション 8 に記載されているすべての機能が使用できなくなり、すべてのセキュアレジスタは RAZ/WI となります。GTZC は、特権アクセスを設定するために引き続き使用できます。

TZEN = 1 から TZEN = 0 への解除後、サンプルは生産状態に相当する未使用状態になります。

注 STM32L5 の場合のみ、BOOT_LOCK オプションビットがセットされている場合、それはクリアできません。TZEN をクリアして再度セットした後、BOOT_LOCK はセットされたままであり、固有のブートエントリアドレスは SECBOOTADD0[24:0] オプションバイトにプログラムされたアドレスになります。

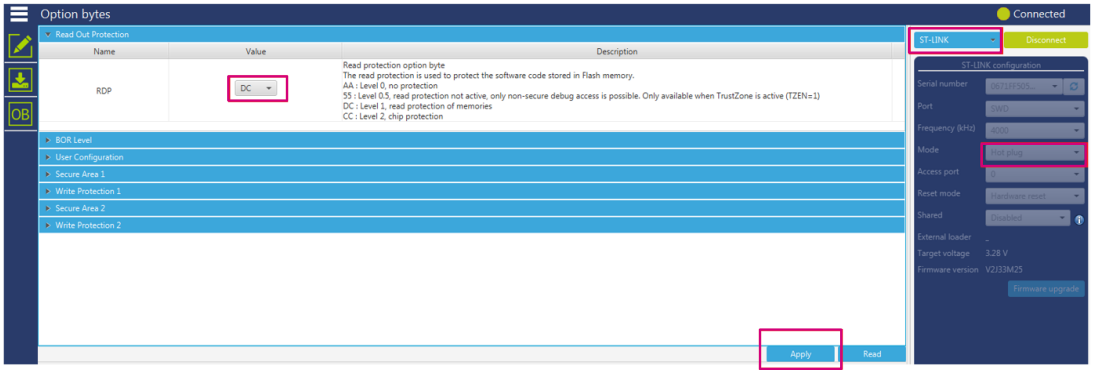
## 9.1 STM32CubeProgrammer を使用した TrustZone/RDP の無効化のデモ

### 9.1.1 ユーザ Flash メモリからのブートによる TZEN/RDP の解除

ユーザ Flash メモリからのブートで TZEN および RDP の解除を実行するには、次の手順が必要です。

1. セキュアアプリケーションと非セキュアアプリケーションが適切にロードされ、実行されることを確認します。
2. STM32CubeProgrammer を使用して（侵入検知が発生します）、RDP をレベル 1（STM32L5 の場合はレベル 0.5）に設定します。この場合、「ホットプラグ」接続のみが可能です。

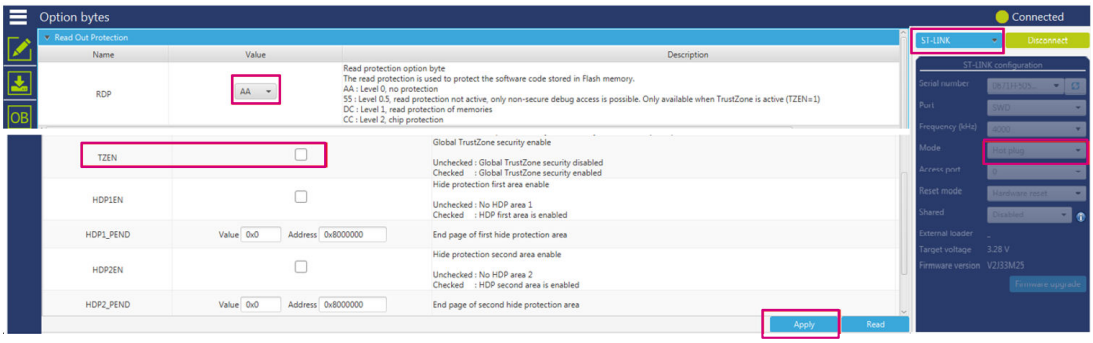
**図 8. RDP をレベル 1 に設定**




3. 侵入検知状態から回復するには、次のいずれかの代替手段を選択します。
   a. ターゲットに接続できるようにするために、ST-LINK とは異なる電源を使用してください（詳しくはセクション 7.1 を参照）。
   b. IDD ジャンパを取り外してから、元に戻し、侵入検知状態から抜けます。

4. RDP をレベル 0（オプションバイト値 0xAA）に設定し、TZEN ボックスのチェックを外し、Apply（適用する）をクリックします。

**図 9. ユーザ Flash からのブートを使用した SWD による TZEN および RDP の解除**




ユーザ Flash からのブートによる TZEN および RDP の解除が、最初のステップを守らなかった（セキュアアプリケーションが非セキュアアプリケーションをコールしなかった）ために成功しなかった場合、解除を行う唯一の方法は、次のセクションで示すように RSS からブートすることです。

### 9.1.2 RSS からのブートによる TZEN/RDP の解除

このセクションでは、STM32L5/U5 ST ボードでのブートの変更方法について説明します。

ブートは、BOOT0 ピンにハイレベルを与えることによって、RSS から実行する必要があります。

- 評価ボード（STM32L552E-EV または STM32U575I-EV）では、ブートを変更するためのスイッチ SW1 が備えられています（文書 [4] または [5] を参照）。
- Discovery キット（STM32L562E-DK または B-U585I-IOT02A）では、ブートを RSS から変更するために、小さな手直しを行う必要があります（文書 [6] または [7] を参照）。
- Nucleo ボード（NUCLEO-L552ZE-Q または NUCLEO-U575ZI-Q）では、CN11 のピン 5（VDD）とピン 7（PH3_BOOT0）間の接続を行う必要があります（文書 [8] または [9] を参照）。

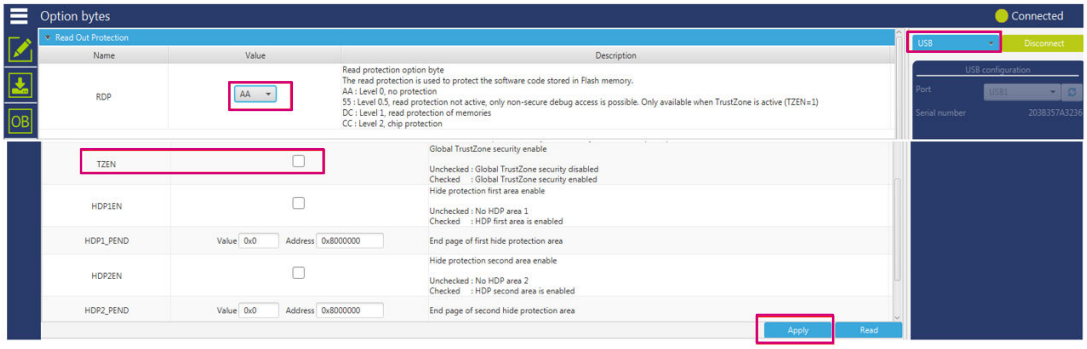
RSS からブートするには、以下の手順を推奨します。

1. 以下の処置が完了していることを確認します。
   a. nSWBOOT0 オプションバイトをチェックします（PH3/BOOT0 ピンから取得した BOOT0）。
   b. PH3/BOOT0 ピンにハイレベル電圧を印加します。
   c. NSBOOTADD1 オプションバイトは、0x0BF9 0000 アドレス（RSS アドレス）で 0x17F200 の値に設定します。
   d. BOOT_LOCK オプションバイトはチェックを外します（パッド／オプションビット設定に基づいてブートされます）。
2. STM32CubeProgrammer で RDP をレベル 1 に設定します（侵入検知が発生します）。この場合、「ホットプラグ」接続のみが可能です。
3. 次の代替方法のいずれかを使用して、侵入検知状態から回復します。
   a. IDD ジャンパを取り外してから、元に戻し、侵入検知状態から抜けます。
   b. ターゲットに接続できるようにするためには、ST-LINK とは異なる電源を使用してください。
4. RDP をレベル 0（オプションバイト値 0xAA）に設定し、TZEN ボックスのチェックを外します。Apply（適用する）をクリックします。

解除は、以下に説明するように、JTAG/SWD またはブートローダを介して実行できます。

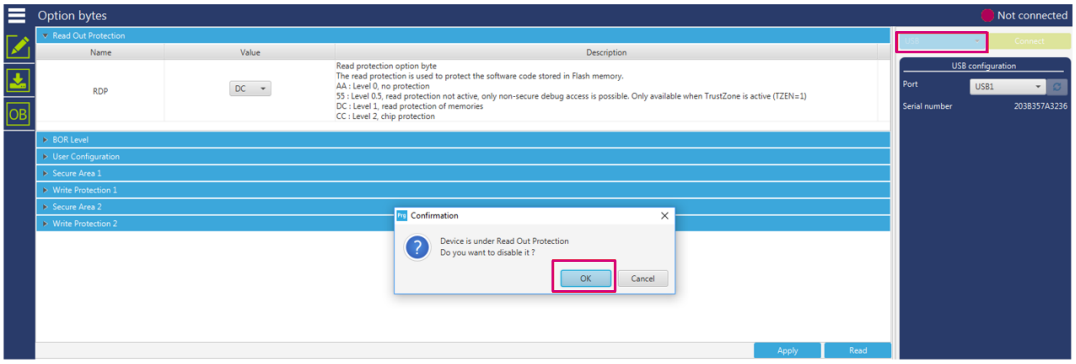
- JTAG/SWD で、RDP をレベル 0（オプションバイト値 0xAA）にセットし、TZEN ボックスのチェックを外し、Apply（適用する）をクリックします。
- ブートローダから、サポートされている通信インタフェースの 1 つ（この例では USB）を使用し、
  - RDP がレベル 0.5 に設定されている場合、RDP レベルをレベル 0（オプションバイト値 0xAA）に設定し、TZEN ボックスのチェックを外し、Apply（適用する）をクリックします。
    注：RDP レベル 0.5 からレベル 0 への解除は、STM32L5 でのみ可能です。STM32U5 の場合、RDP のレベルは、最初にレベル 0.5 からレベル 1 に上げ、次に、TZEN の無効化と並行して、レベル 1 からレベル 0 に戻す必要があります。

**図 10. ブートローダによる TZEN および RDP の解除（レベル 0.5 からレベル 0 へ）**




- RDP がレベル 1 に設定されている場合の、STM32CubeProgrammer グラフィカルインタフェースを使用した RDP 解除を下の図に示します。

**図 11. ブートローダによる RDP 解除（レベル 1 からレベル 0 へ）**




RDP がレベル 1 に設定されていて、STM32CubeProgrammer グラフィカルインタフェースを使用して TZEN 解除を実行できない場合、STM32CubeProgrammer CLI（コマンドライン命令）を使用して、次の TZEN 解除コマンドを適用する必要があります。

```
> STM32_Programmer_CLI.exe -c port=USB1 -tzenreg
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------
USB speed   : Full Speed (12MBit/s)
Manuf.ID    : STMicroelectronics
Product ID  : DFU in FS Mode
SN          : 207E31953536
FW version  : 0x011a
Device ID   : 0x0482
Warning: Device is under Read Out Protection
Disabling TrustZone...
Disabling TrustZone successfully
```

### 9.1.3 RDP レベル 1 が OEM1 キーによってロックされている場合の TZEN/RDP の解除

この機能 は STM32U5 シリーズでのみ使用可能です。OEM1LOCK ビットがセットされると、OEM1 RDP ロックメカニズムがアクティブになります。これによって、RDP レベル 1 から RDP レベル 0 の解除がブロックされます。

OEM1 キーによる RDP レベル 1 のロックは、次の例の CLI コマンドで行うことができます。ここで、OEM1 の LSB キー [31:0] は 0xABCDEFAB で、OEM1 の MSB キー [63:32] は 0x12345678 です。

```
>STM32_Programmer_CLI.exe -c port=swd  mode=hotplug  -lockRDP1 0xABCDEFAB 0x123456
78
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

    Lock RDP1 password successfully done
```

RDP レベルを 1 に上げるには、次の CLI を使用します。

```
>STM32_Programmer_CLI.exe -c port=swd  mode=hotplug  -ob rdp=0xDC
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

    Option Bytes successfully programmed
```

セクション 2.1 で説明されているように、TZEN の無効化は、RDP レベル 1 と並行に実行する必要があります。RDP レベル 1 の解除をアンロックするには、OEM1 キーを指定する必要があります。OEM1 キーを使って、TZEN の解除 と RDP のレベル 1 からレベル 0 への解除を行うためには、次の STM32CubeProgrammer の CLI を使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=UR -unlockRDP1 0xABCDEFAB 0x12345678 -
ob RDP=0xAA TZEN=0
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------

    Unlock RDP1 password successfully done
    Option Bytes successfully programmed
```

# 10 OEM キーを使用した RDP 遷移のデモ(STM32U5 のみ)

最高の保護レベルに達するためには、TrustZone を有効化し、パスワード認証による解除を有効にして RDP レベル 2 を設定することをお勧めします。

RDP は、Flash メインメモリ、オプションバイト、バックアップレジスタ、バックアップ RAM(STM32U5 のみ)、OTFDEC 領域(使用できる場合)、ICACHE、DCACHE、SRAM を保護します。2 つの 64 ビットキー(OEM1KEY および OEM2KEY)を定義して、RDP 解除をロックできます。TrustZone がアクティブ化されると、前のセクションで説明した一連の保護により、CPU はセキュアゾーンと非セキュアゾーンに分割されます。

このセクションでは、RDP 解除をアンロックするために OEM1KEY と OEM2KEY がプロビジョニングされた場合に、STM32CubeProgrammer CLI を使用して RDP レベルの遷移を実践する方法を示します。

注 OEMxKEY を使用した RDP の遷移の詳細については、文書 [2] を参照してください。

この例では、CPU がセキュアであるときに、RSS によって RDP 解除を行います。これは、PH3_BOOT0 ピンをボード上で VDD に接続することによって実行できます。次の表に、最初の列からリンクしているセクションで詳しく述べている遷移手順を要約します(CPU が非セキュアのとき、レベル 0.5 への/からの遷移を除き、これらの手順はすべて適用可能です)。

**表 10. OEMxKEY を使用した RDP 遷移のデモ手順**

| ステップ番号とタイトル | 説明 | コメント |
|---|---|---|
| ステップ 1 - OEM1KEY のプロビジョニング | RDP1 から RDP0 への解除をアンロックするための OEM1Key をプロビジョニングします<br>(`OEM1KEY=0x11ABCDEF 0x12ABCDEF`)。<br>。 | ユーザは、すべて 1 またはすべて 0 を除いて、任意の 64 ビット長のキーを選択できます。`0xFFFFFFFF 0xFFFFFFFF` を使用すると、OEMxKEY がクリアされます。 |
| ステップ 2 - OEM2KEY のプロビジョニング | 次のために OEM2Key をプロビジョニングします<br>(`OEM2KEY=0x21ABCDEF 0x22ABCDEF`)。<br>• RDP2 から RDP1 への解除を許可するため<br>• RDP1 から RDP0.5 への解除をアンロックするため | |
| ステップ 3 - OEMxKEY がプロビジョニングされているかどうかの確認 | OEM1LOCK および OEM2LOCK ビットが 1 にセットされます。 | OEMxKEY が適切にプロビジョニングされていない場合、ユーザーは失敗したステップ 1 またはステップ 2 を繰り返し、再度確認する必要があります。 |
| ステップ 4 - オプションバイト TZEN = 1 をセット | CPU をセキュアに設定します。 | TrustZone が有効になります。 |
| ステップ 5 - RDP レベル 2 の設定 | RDP をレベル 2 に上げます(`-ob rdp=0xCC`)。<br>これは、OEM2KEY が供給されたときに、RDP レベル 2 からレベル 1 への解除が許可されることを示します。 | ステップ 2 を確実に成功させてください。そうでないと、デバイスにアクセスできなくなります。 |
| ステップ 6 - OEM2Key を使用して RDP レベル 2 をアンロック | RDP レベル 2 からレベル 1 への解除を許可します。<br>正しい OEM2KEY を指定する必要があります。 | • アンダーリセット(UR)モードが必要です。<br>• TZEN = 1 の場合、RSS からのブートが必要です。 |
| ステップ 7 - RDP をレベル 1 に設定 | RDP のレベル 1 への解除が可能になりました(ステップ 6 でアンロック済み)。 | 成功しなかった場合は、RDP レベル 2 からレベル 1 への解除が、正しい OEM2KEY でアンロックされていないことを意味します。 |
| ステップ 8 - OEM2 キーを使用して RDP レベル 1 をアンロック | RDP レベル 1 からレベル 0.5 への解除を有効にします。 | CLI でオプション `-unlockrdp1` が `OEM2KY=0x21ABCDEF 0x22ABCDEF` とともに使用されていることを確認します。 |
| ステップ 9 - RDP レベル 0.5 の設定 | ステップ 8 で OEM2Key が提供されているため、RDP レベル 1 からレベル 0.5 への解除が可能になりました。 | - |
| セクション 10.10 ステップ 10 - RDP をレベル 0.5 からレベル 1 に上げる | - | RDP レベル 0.5 からレベル 0 への解除はできないので、ユーザはまず RDP をレベル 1 まで上げる必要があります。 |
| セクション 10.11 ステップ 11 - OEM1Key を使用して RDP レベル 1 をアンロック | 正しい OEM1KEY を指定する必要があります。 | - |

| ステップ番号とタイトル | 説明 | コメント |
|---|---|---|
| ステップ 12 - RDP レベル 0 を設定し、TZEN = 0 にリセット | TZEN + RDP レベル 1 からレベル 0 への解除 | - |

## 10.1 ステップ 1 - OEM1KEY のプロビジョニング

RDP レベル 1 からレベル 0 への解除をロックするために OEM1KEY(0x11ABCDEF 0x12ABCDEF)をプロビジョニングします。次のコマンドラインを使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -lockrdp1 0x11ABCDEF 0x12ABCDE
F
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x30
Debug in Low Power mode enabled
Lock RDP1 password successfully done
```

## 10.2 ステップ 2 - OEM2KEY のプロビジョニング

RDP レベル 2 からレベル 1 への解除を許可するため、または RDP レベル 1 からレベル 0.5 への解除をロックするために、OEM2KEY(0x21ABCDEF 0x22ABCDEF)をプロビジョニングします。次のコマンドラインを使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -lockrdp2 0x21ABCDEF 0x22ABCDE
F
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x20
Debug in Low Power mode enabled
Lock RDP2 password successfully done
```

## 10.3 ステップ 3 - OEMxKEY がプロビジョニングされているかどうかの確認

FLASH_NSSR レジスタの OEM2LOCK および OEM1LOCK ビットがセットされていることを確認して、OEM1KEY/OEM2KEY がプロビジョニングされ、ロックされていることを確認します。次のコマンドラインを使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -r32 0x40022020 4
Reading 32-bit memory content
  Size          : 4 Bytes
  Address:      :0x40022020

0x40022020 : 000C0000   --> FLASH_NSSR[19:18]=11
```

GUI を使用して、アドレス 0x40022020 のメモリまたは Flash_NSSR レジスタの内容を確認します。

## 10.4 ステップ 4 - オプションバイト TZEN = 1 をセット

TrustZone を有効にするには、次のコマンドを使用して TZEN オプションバイトをプログラムします。

```
>STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob TZEN=1

UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x50022040
  Size           : 32 Bytes
[##################################################] 100%
  Bank           : 0x01
  Address        : 0x50022060
  Size           : 8 Bytes
[##################################################] 100%
  Bank           : 0x02
  Address        : 0x50022068
  Size           : 8 Bytes
[##################################################] 100%
OPTION BYTE PROGRAMMING VERIFICATION:
Option Bytes successfully programmed
```

## 10.5 ステップ 5 - RDP レベル 2 の設定

次のコマンドでオプションバイトを設定して(`-ob rdp=0xCC`)、RDP をレベル 2 に上げます。

```
>STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob rdp=0xCC


UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x50022040
  Size           : 32 Bytes
[##################################################] 100%
  Bank           : 0x01
  Address        : 0x50022060
  Size           : 8 Bytes
[##################################################] 100%
  Bank           : 0x02
  Address        : 0x50022068
  Size           : 8 Bytes
[##################################################] 100%
PROGRAMMING OPTION BYTES AREA ...
  Bank           : 0x00
  Address        : 0x50022040
  Size           : 32 Bytes
[                                                  ]
Reconnecting...
Error: failed to reconnect after reset !
UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes
[                                                  ]
Error: Uploading Option Bytes bank: 0 failed
Error: Reloading Option Bytes Data failed  --> Not possible to reconnect as RDP2
```

## 10.6 ステップ 6 - OEM2Key を使用して RDP レベル 2 をアンロック

RDP レベル 2 から RDP レベル 1 への遷移を許可するために、OEM2KEY を提供します。

注 アンダーリセットモード(UR)を推奨します。

次のコマンドを使用します。

```
>STM32_Programmer_CLI.exe -c port=swd mode=UR -unlockrdp2 0x21ABCDEF 0x22ABCDEF
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------
ST-LINK SN  : 0028003D3038510234333935
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZE
Voltage     : 3.31V
Unlock RDP2 password succefully done!
Error: Cannot connect to access port 0
If you are trying to connect to a device with TrustZone enabled please try to conn
ect with HotPlug mode
```

問題が発生した場合は、

- RSS からシステムがブートすること、およびボードの PH3-BOOT0 ピンが VDD に接続されていることを確認してください。
- 次のコマンドを使用して、DBGMCU に RDP レベル 2 でアクセスできること(DBGMCU_CR @0xE0044000)を確認してください。

```
>STM32_Programmer_CLI.exe -c port=swd mode=hotplug -r32 0xE0044104 4
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x20
Debug in Low Power mode enabled
Reading 32-bit memory content
  Size          : 4 Bytes
  Address:      :0xE0044104

0xE0044104 :292D8E4A
```

DBGMCU にアクセスできない場合、OEM2KEY がプロビジョニングされなかったことを意味します。

## 10.7 ステップ 7 - RDP をレベル 1 に設定

次のコマンドを使用して、RDP レベル 2 からレベル 1 への解除(ステップ 6 で OEM2KEY によってアンロックされた)を起動します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob rdp=0xDC
….
UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes
[##################################################] 100%
  Bank           : 0x01
  Address        : 0x40022060
  Size           : 8 Bytes
[##################################################] 100%
  Bank           : 0x02
  Address        : 0x40022068
  Size           : 8 Bytes
[##################################################] 100%
OPTION BYTE PROGRAMMING VERIFICATION:
Option Bytes successfully programmed
```

## 10.8 ステップ 8 - OEM2 キーを使用して RDP レベル 1 をアンロック

RDP レベル 2 から RDP レベル 1 および RDP レベル 1 から RDP レベル 0.5 への解除を許可するために、OEM2KEY をプロビジョニングします。2 番目の場合は、次のコマンドを使用して、OEM2KEY（`0x21ABCDEF 0x22ABCDEF`）で RDP レベル 1 をアンロックする必要があります。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -unlockrdp1 0x21ABCDEF 0x22ABC
DEF
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.8.0
      -------------------------------------------------------------------
ST-LINK SN  : 0028003D3038510234333935
ST-LINK FW  : V3J8M3
Board       : NUCLEO-U575ZE
Voltage     : 3.31V
SWD freq    : 24000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x482
Revision ID : Rev B
Reconnecting with the recommended frequency (1000 kHz)!
…
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x90
Debug in Low Power mode enabled

Unlock RDP1 password successfully done
```

## 10.9 ステップ 9 - RDP レベル 0.5 の設定

次のコマンドを使用して、RDP レベル 1 からレベル 0.5 への解除（ステップ 8 で OEM2KEY によってアンロックされた）を起動します。

```
>STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob rdp=0x55
….
UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes
[##################################################] 100%
  Bank           : 0x01
  Address        : 0x40022068
  Size           : 8 Bytes
[##################################################] 100%
OPTION BYTE PROGRAMMING VERIFICATION:
Option Bytes successfully programmed
```

## 10.10 ステップ 10 - RDP をレベル 0.5 からレベル 1 に上げる

次のコマンドを使用して、RDP をレベル 1 に上げ、次のステップで RDP レベル 0 に到達できるようにします（RDP レベル 0.5 から 0 への遷移は許可されていません）。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob rdp=0xDC
….
UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes
[##################################################] 100%
  Bank           : 0x01
  Address        : 0x40022068
  Size           : 8 Bytes
[##################################################] 100%
OPTION BYTE PROGRAMMING VERIFICATION:
Option Bytes successfully programmed
```

## 10.11 ステップ 11 - OEM1Key を使用して RDP レベル 1 をアンロック

正しい OEM1KEY を指定する必要があります。そうしないと、解除はできません。次のコマンドで、RDP レベル 1 をアンロックします。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -unlockrdp1 0x11ABCDEF 0x12ABC
DEF
…
Reconnected with the recommended frequency (3300 kHz)!
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0xf0
Debug in Low Power mode enabled

Unlock RDP1 password successfully done
```

## 10.12 ステップ 12 - RDP レベル 0 を設定し、TZEN = 0 にリセット

TrustZone が有効になっている場合、TZEN オプションバイトの無効化は、RDP レベル 1 からレベル 0 への解除と同時に行う必要があります。次のコマンドを使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob rdp=0xAA tzen=0
….
UPLOADING OPTION BYTES DATA ...
  Bank           : 0x00
  Address        : 0x40022040
  Size           : 32 Bytes
[##################################################] 100%
  Bank           : 0x01
  Address        : 0x40022068
  Size           : 8 Bytes
[##################################################] 100%
OPTION BYTE PROGRAMMING VERIFICATION:
Option Bytes successfully programmed
```

注 TrustZone が無効になっている場合は、コマンドは次のとおりです。

```
STM32_Programmer_CLI.exe -c port=swd mode=hotplug -ob rdp=0xAA
```

## 10.13 OEMxKEY のクリア

OEM1KEY と OEM2KEY の両方の Flash メモリオプションバイトに `0xFFFFFFFF 0xFFFFFFFF` を書き込むことによって、OEM1Key および/または OEM2KEY をクリアします。

その結果、Flash_NSSR [19:18] の OEM1_LOCK および／または OEM2_LOCK ビットがクリアされます。これらは、セクション 10.3 で述べたようにして確認できます（Flash_NSSR [19:18] = 00）。

注意 OEM2KEY がクリアされているか、まったくプロビジョニングされていない場合、RDP レベル 2 からレベル 1 への解除はできません。

ステップ 1（セクション 10.1）とステップ 2（セクション 10.2）のように 、最初に OEM1 および OEM2 キーにキーがプロビジョニングされた場合、

- OEM1key は、RDP レベル 0 でクリアできます。
- OEM2Key は、RDP レベル 1、レベル 0.5、またはレベル 0 でクリアできます。

### OEM1KEY のクリア

STM32CubeProgrammer CLI インタフェースで次のコマンドを使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -lockrdp1 0xFFFFFFFF  0xFFFFFF
FF
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x30
Debug in Low Power mode enabled
Lock RDP1 password successfully done
```

### OEM2KEY のクリア

次のコマンドを使用します。

```
> STM32_Programmer_CLI.exe -c port=swd mode=hotplug -lockrdp2 0xFFFFFFFF  0xFFFFFF
FF
Device name : STM32U575/STM32U585
Flash size  : 2 MBytes
Device type : MCU
Device CPU  : Cortex-M33
BL Version  : 0x30
Debug in Low Power mode enabled
Lock RDP2 password successfully done
```

ユーザは、ステップ 3（セクション 10.3）で説明したように、FLASH_NSSR レジスタの内容を読み出すことによって、OEM1LOCK および OEM2LOCK ビットがクリアされたことを確認できます。

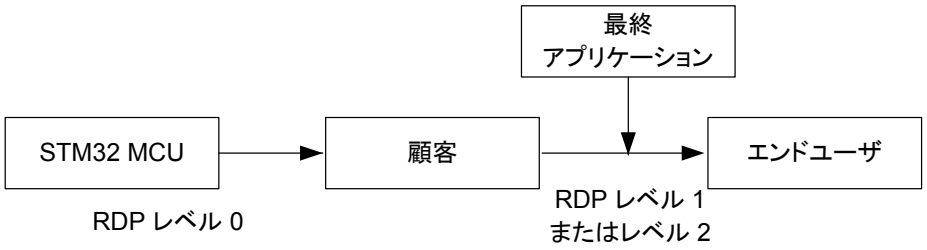
# 11 TrustZone を使用した開発の推奨事項

## 11.1 開発アプローチ

開発には 2 つの開発者アプローチがあります。

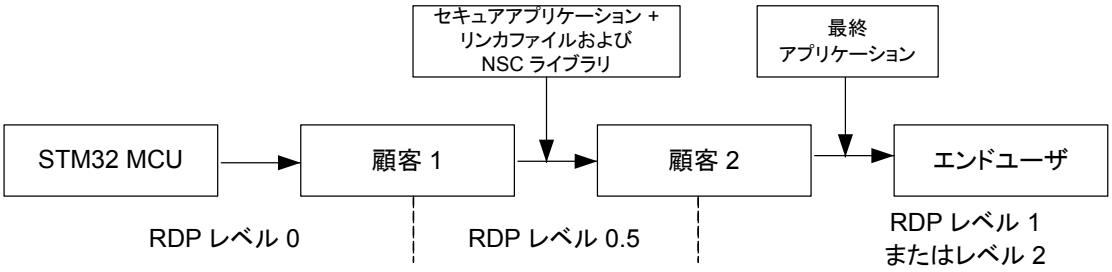
- 単一開発者によるアプローチ：開発者（顧客）は、セキュアアプリケーションと非セキュアアプリケーションの開発を担当します。ユーザアプリケーションは、RDP レベル 1 または RDP レベル 2 を使用して保護できます。

**図 12. 単一開発者によるアプローチ**




- デュアル開発者によるアプローチ：最初の開発者（顧客 1）は、セキュアアプリケーションとそれに関連する非セキュアから呼出し可能ライブラリ（.lib/.h）を作成し、非セキュアアプリケーションの開発を担当する 2 番目の開発者（顧客 2）に事前定義されたリンカファイルを提供することを担当します。そして、このセキュアアプリケーションを STM32L5/U5 のセキュア Flash メモリにロードし、RDP レベル 0.5 を使用して保護し、デバイスのセキュアメモリ領域にそれ以上アクセスされないようにします。その後、2 番目の開発者（顧客 2）は、顧客 1 から提供されたリンカファイルと非セキュアから呼出し可能ライブラリを使用して、事前にプログラムされた STM32L5/U5 上で開発を開始します。
  RDP レベルがレベル 0.5 に設定された場合、セキュア Flash メモリ部分をプロビジョニングする顧客 1 は、セキュア側でブートした後に非セキュア側（顧客 2）のために JTAG/SWD を有効にする方法についても考慮する必要があります。.このため、顧客 1 は、非セキュア Flash メモリに引き継ぐスイッチ機能を実装して、顧客 2 が非セキュア部分を開発できるようにする必要があります。また、場合によっては、デバイスを RDP レベル 1 またはレベル 2 にロックする必要があります。

**図 13. デュアル開発者によるアプローチ**




詳細については、文書 [1] または [2] の「製品ライフサイクル」および「ソフトウェアの知的財産の保護と共同開発」のセクションを参照してください。

## 11.2 非セキュアペリフェラルの使用

ペリフェラルが非セキュアワールドに割り当てられると、セキュアアプリケーションと非セキュアアプリケーションの両方がペリフェラルレジスタにアクセスできます。

非セキュアワールドでは、Armv8-M の TrustZone の考慮事項は開発者に対して完全に透過的です。セキュアワールド側では、アプリケーションは、ペリフェラルが必要とするすべてのシステムリソースを事前に設定しておくか、または非セキュアワールド側（GPIO、NVIC、または DMA など）が使用できるようにしておく必要があります。

## 11.3 セキュアペリフェラルの使用

ペリフェラルがセキュアワールドに割り当てられた場合、セキュアレジスタアクセスのみが許可されます。割込み処理はセキュアワールドでのみ行う必要があります。このペリフェラルを使用するためのセキュアおよび非セキュアプロジェクト間のソフトウェア相互作用の要件に応じて、2 つの異なるソフトウェア開発アプローチを採用できます。

非セキュアワールドとの特定の相互作用を必要としないペリフェラルを使用する場合、セキュアワールドでは、特別な考慮事項なしに、これらのペリフェラルを標準ペリフェラルとして駆動します。

セキュアペリフェラルを駆動するために非セキュアワールドとセキュアワールドの間の相互作用が必要な場合、セキュアアプリケーションは、非セキュアから呼出し可能 API とコールバックを非セキュアワールドに提供する必要があります。

# 12 結論

Arm TrustZone テクノロジーでは、ハードウェアをセキュアと非セキュアワールドに分割します。

ユーザ設定可能な SAU とともに固定のメモリマップセキュリティ属性を定義する IDAU 、および（Flash メモリおよび GTZC にある）その他の機能により、すべての STM32 マイクロコントローラリソース（メモリマップ、Flash メモリ、SRAM、外部メモリ、ペリフェラル、およびペリフェラル割込みを含む）はセキュアワールドと非セキュアワールドのどちらにも設定できます。

# 改版履歴

表 11. 文書改版履歴

| 日付 | 版 | 変更内容 |
|---|---|---|
| 2019 年 10 月 11 日 | 1 | 初版発行 |
| 2019 年 10 月 14 日 | 2 | 図 6. メモリおよびペリフェラルのデータアクセスルールの概要を更新。 |
| 2019 年 2 月 10 日 | 3 | 更新:<br>• 概要<br>• セクション 2.1 概要<br>• セクション 2.2 セキュリティ状態<br>• セクション 3.1 STM32L5 シリーズの TrustZone のアクティブ化<br>• セクション 3.3 SAU および IDAU<br>• 図 3.アドレスセキュリティ属性<br>• セクション 3.3.1 STM32L5 シリーズの IDAU とメモリのエイリアス化<br>• 表 1.STM32L5 シリーズでの IDAU メモリマップアドレスセキュリティ属性<br>• セクション 3.3.2 STM32L5 シリーズの SAU<br>• セクション 4 STM32L5 シリーズデバイスのセキュリティ設定<br>• セクション 4.1 Flash メモリのセキュリティ設定<br>• セクション 4.1.1 Flash メモリのセキュアウォーターマーク<br>• セクション 4.1.2 Flash メモリブロックベース<br>• セクション 5.1 デフォルトのセキュリティ状態<br>• セクション 5.2 メモリとペリフェラルのセキュリティアクセスルール<br>• 図 6.メモリおよびペリフェラルのデータアクセスルールの概要<br>• セクション 6 ブートおよびルートセキュアサービス（RSS）<br>• セクション 7.1 RDP レベル 1 および セクション 7.2 RDP レベル 0.5<br>• セクション 8 TrustZone が有効な場合にのみ使用可能なセキュリティ機能<br>• セクション 9 TrustZone の無効化<br>• セクション 10.1、セクション 10.2、およびセクション 10.3<br>• セクション 11 結論<br>追加:<br>• セクション 1.1 参考文書<br>• 図 5.オプションバイトによるデフォルトの Flash バンクのセキュリティ状態<br>• 表 4.命令フェッチルール<br>• セクション 10 TrustZone を使用した開発の推奨事項 |
| 2020 年 3 月 2 日 | 4 | 更新:<br>• セクション 7.1 RDP レベル 1<br>• セクション 7.2 RDP レベル 0.5<br>セクション 9.1 STM32CubeProgrammer を使用した TrustZone/RDP の無効化のデモを追加。 |
| 2021 年 9 月 28 日 | 5 | 更新:<br>• STM32U5 シリーズを統合するためのタイトルおよび全文<br>• セクション 1 一般情報の参照文書<br>• セクション 3.3.2 STM32L5 および STM32U5 の SAU<br>• セクション 4 STM32L5 および STM32U5 シリーズのセキュリティ設定<br>• セクション 7 TrustZone が有効な場合の読出し保護（RDP）<br>• セクション 8 TrustZone が有効な場合にのみ使用可能なセキュリティ機能<br>• セクション 9.1.2 RSS からのブートによる TZEN/RDP の解除<br>• セクション 11.1 開発アプローチ<br>追加:<br>• セクション 7.3 RDP レベル 2<br>• セクション 7.4 OEM キーを使用した RDP 遷移（STM32U5 のみ）<br>• セクション 9.1.3 RDP レベル 1 が OEM1 キーによってロックされている場合の TZEN/RDP の解除<br>• セクション 10 OEM キーを使用した RDP 遷移のデモ（STM32U5 のみ） |
| 2022 年 4 月 8 日 | 6 | 更新:<br>• 各種誤記 |

# 目次

# 表一覧

# 図一覧